idealintegrations
building networks and partnerships

Incident Response Lead

The Incident Response lead will be responsible for the implementation of security solutions during an Incident. The desired candidate will be a subject matter expert in all core technical solutions which the security operations center (SOC) offers. The desired candidate would assist in any Security related activities of the entire Incident Response lifecycle. The desired candidate will have excellent customer facing skills. The desired candidate will allocate time to finding new solutions for those issues which may arise in the security department. The desired candidate must document all situations accurately and completely. The desired candidate must possess strong verbal skills to convey information accurately to clients, and for the training of SOC members.

Principle Accountabilities:

- Day to day responsibilities including:
  - Coordinate and lead investigations and response activities with IR analysts
  - Work with and coordinate response activities with infrastructure team(s) involved in recovery activities
  - Coordinate and lead forensics acquisition efforts
  - Ensure all time spent is appropriately placed into the IR management solution on the security side
  - Participate in the creation, and maintenance Incident Response Standards, Policies, Procedures, Guidelines, and Checklists
  - Provide feedback to current process, procedures, and find ways to actively become better
  - Hold Post-Incident reviews to ensure that we continue to improve
  - Collecting all IOCs into a single location to ensure we can re-use these IOCs
  - Creating scripts, tools, and/or methods to enhance current services and processes
- When not doing IR actively, or the responsibilities above:
  - Help Threat Hunting engagements across all clients
  - Help develop new automated ways to threat hunt clients
  - Create, and provide training to Analysts, Engineers, etc. for how to improve current services
  - Threat Research that is pushed out to the team
  - Mentor SOC staff

Other Accountabilities:

- Respond to Alerts, events, and incidents per our specified procedures and processes
- Log and record all alerts with ticketing system
- Identify weaknesses in customer infrastructures and suggest improvements
- Technical and analytical skills to handle security events, incidents, and threats
- Resolve events and incidents
- Provide timely and reliable service to customers
- Stay up to date on latest vulnerabilities exploits and any other relevant threat information
- Operation, implementation, and maintenance of security solutions
- Document solutions, processes, or procedures in written, verbal, phone, or in person.
- Requirement for on-call work
- Ability to work in a very fast-paced environment
- Assist in creation and maintenance of documentation for SOC procedure and processes

- Ensuring they are complying with and adhering to all Information Security Policies as well as privacy policies. They must also ensure they are protecting and keeping secure all client information considered or believed to be private or sensitive.
- Ensuring all security and operational controls are followed and enforced to ensure client data remains secure, available, and private, where applicable.

Experience/Skills:

- Knowledge of:
    - Incident Response Methodologies, and experience in Incident Response
    - Threat Analysis
    - Threat identification
    - Direct system remediation
    - Experience with EDR solutions
    - Experience with log collection
    - Experience in running high stress incident calls
    - Experience in creating plans for malware eradication
- Incident Response / SOC / Blue team experience / Red Team experience
- Programming / Shell scripting experience (PERL, Python, Java, Shell, PowerShell, etc.)
- Experience as a System Admin, or Network Administrator
- Knowledge of configuring and implementing technical security solutions (Firewalls, IDS/IPS, Antivirus, SIEM, etc.)
- Strong desire to constantly learn
- Customer –oriented focus with a strong interest to satisfy our customers
- Solid understanding of networking and security
- Knowledge of Windows Operating systems applications
- Knowledge of Linux Operating Systems and applications
- Knowledge of Incident Response lifecycles and standards
- Knowledge of Penetration Testing Operating Systems and applications
- Understanding varying Security standards PTES, Defense in Depth, etc.
- One or more of the following certifications preferred: CFCE, CCE, GCFA, GCFE, GNFA, FREM, FASF, GCIH, EnCE, and ACE

Additional Information

- Preferred Education: Minimum of Technical or Associate degree in a relevant field or equivalent professional experience.
- Some travel and heavy lifting may be required.

Classification Information

- Level/Department: Technical
- Reports to: VP of Security Solutions
- Date Reviewed: 11/10/2022